LEGIBILITY NOTICE

A major purpose of the Technical Information Center is to provide the broadest dissemination possible of information contained in DOE's Research and Development Reports to business, industry, the academic community, and federal, state and local governments.

Although a small portion of this report is not reproducible, it is being made available to expedite the availability of information on the research discussed herein.

1

LA-UR -88-79

LA-UR--88-79

DE88 005376

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE INTEGRATED SAFECUARDS AND FACILITY DESIGN AND OPERATIONS

AUTHOR(S): J. W. Tape, C. A. Coulter, J. T. Markin, and K. E. Thomas

SUBMITTED TO ANS Topical Conference, The 3rd International Conference on Facility Operations Safeguards Interface, San Diegc, November 29-December 4, 1987

Los Alamos

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

FORM NO 836 R4
ST NO 2629 5/81

INTEGRATED SAFEGUARDS AND FACILITY DESIGN AND OPERATIONS

J. W. Tape, C. A. Coulter, J. T. Markin, and K. E. Thomas
Los Alamos National Laboratory
Los Alamos, NM 87545
(505) 667-7777

ABSTRACT

The integration of safeguards functions to deter or detect unauthorized actions by insiders requires careful communication and management of safeguards-relevant information on a timely basis. The separation of safeguards functions into physical protection, materials control, and materials accounting often inhibits important information flows. Redefining the major safeguards functions as authorization, enforcement, and verification and careful attention to management of information can result in effective safeguards integration. Whether designing new systems or analyzing existing ones, understanding the interface between facility operations and safeguards is critical to cost-effective integrated safeguards systems that meet modern standards of performance.

I. INTRODUCTION

Responsible management of nuclear materials, always a difficult task, has become even more challenging in the context of a world that is increasingly averse to nuclear-related risk. Facility operators must constantly provide assurance that their materials are under control and are not being released to the environment or falling into the hands of unauthorized parties. At the same time that societies are demanding the highest standards for nuclear activities, these activities are growing worldwide in applications related to the generation of electricity and are not likely to shrink significantly in military applications. More material is being processed, and there are more facilities responsible for it than ever before. Along with the growth in materials processing, there has been a perceived increase in the human threats posed to nuclear activities. World-wide terrorist activities have motivated government authorities to demand impressive physical protection measures at the perimeters of plants to repel armed attackers. Also, there is a high level of concern regarding malevolent acts by individuals with authorized access to nuclear materials. This insider threat presents the greatest challenge to safeguards system design and operation because it may be much more difficult to distinguish between authorized and unauthorized actions. The components of a safeguards system that can deal with all these threats effectively while interfering minimally with facility operation must be organized into a coherent unit and must emphasize the efficient generation and utilization of safeguards-relevant information.[1,2]

II. INTEGRATED SAFEGUARDS SYSTEMS

A. The Meaning of Integrated Safeguards

The structure and function of domestic nuclear safeguards systems are usually defined in terms of the three concepts of physical protection, materials control, and materials accounting. Although there may be some overlap between the areas of physical protection and materials control, in most instances these three elements of the system function nearly independently of one another, have separate administrative structures, and have few channels of communication with each other. Furthermore, those channels of communication that do exist are normally far removed from the everyday working level and come into play after the fact when an unusual incident has occurred. Duplication of effort and unnecessary interference with facility operation can result from this relatively independent operation of the different parts of the safeguards system, with unnecessarily high safeguards costs as a corollary. In addition, the lack of coordination among the three elements may cause gaps in safeguards systems coverage--particularly with respect to the insider threat--and will almost certainly make it very difficult to evaluate the effectiveness of the total safeguards system.

For these reasons, interest has been growing in the development of integrated safeguards systems. An integrated safeguards system comprises the same basic elements as any other safeguards system: protective personnel, fences, portal monitors, personnel identification systems, process monitors, material measurements, accounting records, and so on. However, the organizational arrangement of these elements is no longer the same. In an integrated safeguards system, the basic safeguards elements are appropriately selected and then combined into a single unit whose parts communicate, share information, cooperate, and coordinate their activities in a manner that is optimized with respect to the dual objectives of achieving maximum safeguards effectiveness and of minimizing interference with facility operations, and without regard to arbitrary classifications such as physical protection, materials control, and materials accounting.

It appears desirable that all safeguards systems be integrated in the sense just described. However, such integration may be difficult or impossible to achieve when the safeguards system is organized along the usual lines of physical protection, materials control, and materials accounting, because this structure compartmentalizes information and provides no avenues for coordinating the actions of units belonging to the different areas. The design and implementation of integrated safeguards systems will therefore require the formulation of new organizational concepts for safeguards systems that encourage rather than hinder the development of integrated systems. In the next two sections we propose that these new concepts should be those of authorization, enforcement, and verification, coupled with the proper collection, analysis, and distribution of information.

B. Safeguards System Functions

One can define domestic nuclear safeguards as a collection of measures intended to assure that nuclear materials are used only in authorized ways for officially approved purposes and to provide effective corrective actions when misuse occurs. This definition contains the elements stated at the end of the last section: authorization for appropriate uses of nuclear materials, enforcement to limit uses to those that are authorized or to detect and terminate misuses, and verification to assure that the facility is in an authorized status, with all these activities necessarily depending on the appropriate acquisition and utilization of information. We shall now discuss the meanings of these terms and concepts more completely and show that they can, in fact, serve as the basis for design and implementation of a nuclear safeguards system.

Authorization in a nuclear facility is a hierarchical definition structure whose purpose is to state precisely at every level what the facility objectives are, what actions are approved for achieving these objectives, what personnel and/or pieces of equipment may perform these actions, and in what manner the actions must be performed. The most effective method for developing the authorization structure for a facility is usually to employ a top-down approach in which the official mission for the facility (often as stated by a government agency) is designated as a top-level task. This top-level task is broken down level by level into required subtasks at successively greater levels of detail until the basic "irreducible" facility activities are reached (for example, performing a particular step of a chemical process, transporting nuclear material from one location to another, and so on). A parallel personnel/equipment structure must then be constructed for the facility, and authority for performing the individual basic activities must be assigned to these facility personnel/equipment resources. Both operational and safeguards considerations will be important in determining the allocation of authorizations to personnel and equipment, but a primary safeguards goal must be to minimize the probability that an unauthorized action can occur without immediate detection and interruption.

Once the authorized activities and personnel have been defined, enforcement methods must be determined to assure that only authorized actions by authorized personnel/equipment occur. Many of these methods fall within the areas usually designated as physical protection and materials control. Barriers and personnel identification systems are used to exclude unauthorized personnel from the facility as a whole or from certain areas of the facility, portal monitors are used to detect attempts at unauthorized transfers of materials, and so on. The enforcement methods must, of course, provide for the interruption of unauthorized activities by force when necessary.

The safeguards verification function continually examines the facility status to ensure that it is within authorized limits. One of the most important verification activities is that of materials accounting, which tries to assure that all nuclear materials are present in their authorized amounts, locations, and forms. Part of the materials accounting verification program is a measurement control program to assure that measuring instruments and processes function correctly. Other instrument verification actions include testing alarm and communication equipment to assure that it is in proper operating condition. In addition, process instrumentation can be monitored for safeguards verification purposes to assure that process parameters are within nominal ranges; material transfers can be monitored to assure that only authorized materials are moved by authorized persons, and that a transfer that has been initiated is completed within an appropriate time period at the correct destination; and so on. Verification activities are very important in the operation of the safeguards system because they can provide positive evidence that the facility is in an authorized status, not just a statement that no unauthorized situations have been detected.

Many of the safeguards system's authorization, enforcement, and verification activities rely extensively on the availability and correct interpretation of information about the system status. Because of the importance and potential complexity of the process of information acquisition, interpretation, and distribution, we discuss this subject separately in the next section.

C. Information Management

Coherent acquisition, organisation, and analysis of safeguards-relevant information is the basis of an integrated safeguards system. This information management system is the framework for continuously acquiring information about facility operations, comparing observed conditions to the anticipated normal conditions, detecting anomalies in routine operations, and implementing procedures for anomaly resolution.

The key elements of information management, acquisition, organization, analysis, and decision-making are described as follows.

Acquisition. Information to be acquired by an integrated safeguards system is determined by its intended use in the analysis, decision-making, and reporting processes that are foreseen. Because this system must counter potential insider threats from personnel authorized for direct access to sensitive material, areas, and information, it must acquire sufficient information to detect subtle deviations from authorized procedures.

Information of potential safeguards use is derived from an understanding of facility operations including material inventories, material flows, and personnel activities for operating the process. Facets of facility operations that are the source of these data are

- <u>Material locations</u> - facility locations where material is stored or temporarily resides including storage vaults, holding areas, and process vessels. Needed information is material amounts, number of items, and typical residence time.
- <u>Material transfers</u> - movements of material between locations in the facility including transfers between process equipment, movements to different locations in a glove box, or transfer between materials balance areas (MBAs). These are defined by source and destination, amount of material, and duration of transfer.
- <u>Process control/monitoring measurement</u> - locations in the facility where process parameters are measured. Defining parameters are location, measurement method, measurement uncertainty, frequency of instrument recalibration, and frequency of measurement.
- <u>Personnel activities</u> - routine personnel activities for operating facility. Specify general job categories and necessary authorizations for personnel access to facility areas, materials, and information.

The basis of information acquisition is a collection of key locations such as measurement points and personnel access control points where safeguards personnel or sensors acquire data on material and personnel activities. These locations are selected in consideration of process operations and a framework of safeguards areas including materials balance areas, material access areas, protected areas, and exclusion zones. The acquisition system parameters are the location, attributes of material or personnel, method of acquisition, and the event that initiates the acquisition.

Integration of the acquisition of information among the various safeguards activities consists of avoiding redundancy and coordinating the acquisition of related data elements. For example, additional safeguards measurements can be eliminated when existing process monitoring measurements are adequate. Also, sensors recording the attributes of transported material and attributes of the custodian should be colocated.

Organization. Traditional separation of safeguards information generated by its various functions limits the range of anomalies that are potentially detectable, whereas integration of these data in a single structure increases the correlations and relations between data that can be examined. For example, confirmation that a material transfer is successfully completed involves the ability to correlate information about material and personnel attributes that is separated in both space and time.

Resolution of anomalies depends on a capacity for rapid recall of related data on past activities involving material and personnel. Retrieval of these data is facilitated when there is an identifying key that associates all data elements related to a particular event. For example, an event involving measurement of an item by an operator generates data such as the item identification, material amount, instrument identification, and operator identity--all perhaps stored in separate data files but easily relatable when tagged with a common unique event number.

The following are examples of database tables that might be maintained:

- access authorizations of each person;
- physical inventory data including location, time, and material amount;
- material transfers across accounting boundaries including location, time, and material amount;
- transactions related to splitting or combining items;
- a record of personnel access requests; and
- nominal process parameters.

Analysis. The function of information analysis in a safeguards system is to reduce the complexity of the data to a simple form that is directly usable by safeguards decision makers. Compression of the information into indicators that are more readily comprehended facilitates discrimination between normal and abnormal conditions in facility operations.

Anomaly detection depends on an analysis of the safeguards information to determine a deviation of an observation from normal facility operations. In some instances these analyses are simple and immediate, as in the comparison of an access request to an authorization list, whereas other analyses such as evaluation of an inventory difference may require large amounts of data and extensive calculations. Analyses may be divided into two classes: statistical analyses such as inventory difference evaluation and logical analyses such as evaluation of an access request.

Statistical analyses are applied to the results of measurements as in analyses of shipper/receiver differences, inventory differences, and measurement of standards to detect instrument malfunction. Examples of data analysis procedures for addressing statistical decision problems, which are often implemented in computer programs, are materials balance closure, variance calculation, materials balance analysis, and measurement control.[4]

Logical analyses deal primarily with comparison of information on personnel activities and material movements and locations with the known normal facility operational procedures to detect anomalies. Currently, these analyses consist of comparisons of personnel area access requests with an authorization database and confirmation that material crossing materials access area boundaries have the appropriate gross attributes. However, as the technology for tracking personnel and material locations advances, more complex authorizations involving sequences of personnel actions and their precise location may become the subject of anomaly detection.

Procedures for logical analysis of safeguards information may consist of programs to retrieve personnel authorization from a database; programs to record the history of personnel accesses to material, areas, and information; and programs to retrieve selected audit trail information.

Decision-making. The final element in developing information management that is consistent with an integrated safeguards system is a decision-making structure consisting of displays of indicators of safeguards status, criteria for determining that an anomaly exists, procedures for resolving anomalies, and personnel responsibilities for the anomaly detection/resolution process.

Indicators presented to a decision maker should constitute the minimum amount of information necessary for resolving the difference between normal and abnormal facility conditions. For each indicator there is an associated criterion for deciding that an anomaly exists. These criteria should be chosen to reflect a desired system sensitivity to an anomaly (for example, amount of material loss to be detected within a specified time and with specified detection probability).

The following indicators are representative of information that could be displayed for decision-making:

- a plot of materials balance sequences for each accounting area with decision thresholds based on variance calculations;
- a listing of the current book inventory in each accounting area;
- a display of material transfers in progress and elapsed time;
- a plot of measurement control charts for each measurement instrument;
- a display of the current access status of personnel to areas, material, and information;
- a display of an audit trail for an item or batch reflecting the processing and measurement history--including personnel access to the material.

The coherent organization, analysis, and display of safeguards information allows the detection of anomalies that are only apparent when data from separate locations, times, and safeguards activities are combined. Examples of anomaly detection based on combined use of information elements are

- repeated evidence of incorrect accounting entries associated with specific personnel;
- a pattern of unauthorized access attempts to areas, material, or information by individuals;
- correlations between large inventory differences and operating shifts;
- a disparity between the material transport authorization of an individual and the material transported;

- a material transfer that is not completed within the allotted time; and
- movement of material at an unauthorized time or to an unauthorized location by an authorized person.

III. FACILITY AND PROCESS DESIGN AND OPERATION —AN EXAMPLE

We now discuss some aspects of designing a facility to meet integrated safeguards objectives. An example facility is used to illustrate several aspects of integrated safeguards; however, all aspects of process operation and safeguards have not been covered in this example, and the example should not be considered a complete and comprehensive design.

The example facility processes high-grade scrap to recover the special nuclear material as oxide. All process operations are performed within glove boxes. The facility has one vault and two process rooms located within the material access area (MAA). The MAA is located within a protected area (PA). The facility layout is illustrated in the Figure.

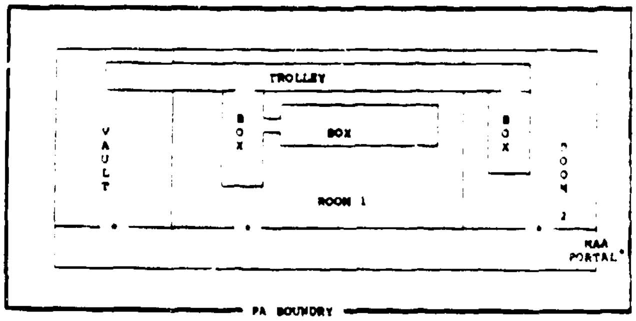

Figure. Example facility layout.

The facility layout has been planned so material and personnel move by different routes. Walls and alarmed doors provide enforcement of authorizations of material movement and personnel access. No material is allowed through personnel portals, therefore any trigger of portal radiation alarms would be investigated immediately as a removal of material.

Process operations occurring in Room 1 are dissolution, ion exchange, and precipitation. All material handling operations in Room 1 are performed on a batch basis. Batch operations facilitate near-real-time accounting by allowing frequent balance closures, and allowing moving (dynamic) inventories by timing inventories to occur when equipment is empty after a batch has completed a process step. This decreases the lost processing time for shutdown inventories and provides more timely verification of the presence of material.

The only process located in Room 2 is calcination, which is operated continuously. A bag-out port is provided in Room 2 but not in Room 1. Because of the loss of batch identity through the calciner and the increased access to material provided by the bag-out port, this operation is isolated from other operations. Fewer people are authorized to have access to this area, and the two-man rule is strictly enforced.

All transfers to and from the vault are by trolley; all transfers within the process rooms are contained within the glove boxes. The two process rooms are connected by trolley. Movement of material is automated, and provision is made for electronically recording the important movement information such as who authorized movement, item identification, time, source, and destination.

We will assume that detailed descriptions of process operations and material movements have been developed for this facility. Portions of the process requiring similar materials and equipment have been located in the same area and physically separated from other areas by appropriate barriers. These detailed descriptions establish authorized locations for materials, authorized transfers, and authorized access to materials. For the example facility, the following authorizations have been approved:

- floor supervisor - authorized for access to all areas, not authorized to access inventory difference information but authorized access to all other information.
- wet process operators - authorized for Room 1 access only, not authorized to access inventory difference or measurement control information but authorized access to all other information; may receive material from the vault but may not send material to the vault.
- calciner operators - authorized for access to Room 2 only, not authorized to access inventory difference or measurement control information but allowed access to all other information; may send material to the vault but may not receive material from the vault.
- safeguards officer - authorized access to all information, but no unescorted access to the MAA.
- health and safety personnel - authorized access to all areas, access to inventory listings, no transfer or material access authorizations.

Special authorizations may be approved as appropriate and granted temporarily for special operations. An authorizations database is compiled from the above information and maintained on the safeguards system by the safeguards officer.

An automated stacker-retriever moves cans within the vault based on requests received from the safeguards or process control computer. All items moving into or out of the vault have been sealed with a tamper indicating device (TID). The stacker-retriever can read the bar code, TID identifier, and load the measurement instruments located within the vault (neutron measurement, gamma spectrometry, weight). Shelf monitors record the constant presence of each item stored in the vault.

Automation of routine tasks such as the vault operation eliminates the need for personnel to have access to material in these areas. Linked with a computer and appropriate measurements, this could be particularly useful by providing information on time of movement, item identification, actions taken, and authorizing person. An added advantage of automation in vaults, or for transfers, is reduced radiation exposure to personnel.

A vault computer records all vault measurement information, shelf monitor data, item positions, and trolley movements; communicates with the safeguards computer; and controls the stacker-retriever. A motion detector within the vault is activated by the vault computer when no activities are scheduled and turned off when a new activity is scheduled. The motion detector sends alarms to the physical protection post as well as to the safeguards computer.

Personnel enter the vault for external shipments of material and for maintenance of equipment. A portal radiation monitor at the door to the vault detects material entering or leaving the vault. Access to the vault is obtained after successful use of a personal identification device by two authorized personnel (authorizations verified by the safeguards computer). All access approvals and records are handled by the access control computer. In addition, if only two personnel are present, the portal monitor is active; therefore, any portal alarm should be responded to as an unauthorized removal of material. For external shipments, a third person must be present, and the safeguards computer must approve deactivation of the portal monitor (for authorized movements of material across the vault portal).

Material is transferred from the vault to Room 1 by trolley. Trolley motion is monitored by computer; starting and stopping position and times are recorded. Once in the process area, the transfer transaction is completed by weighing the item and recording the identifying information. Processing now begins with standard materials accounting in practice. The dried precipitate is transferred to Room 2 by trolley using the same procedure as transfers from the vault to Room 1. This transfer is made using only gross weight and container bar code for the measurements. The precipitate is calcined to oxide, blended, sampled for chemistry measurement, weighed, bar-coded, and sealed in a can with a TID. All of this information is recorded in the accounting system computer. The can is bagged out of the glove box and placed on the trolley for transfer to the vault using the same procedure as transfers from the vault.

Access to process Rooms 1 and 2 is permitted only by successful use of a personal identification device by two personnel for access to the same room. Access to Room 2 may require the presence of three persons due to safety requirements of bag-outs. Because, under normal operating conditions, no material should be transferred manually through the process room portals, portal alarms would be indicative of unauthorized removals of material.

Approval for access to the vault or the process rooms is obtained when the following conditions are met:

1) the individual is on record as having gained access to the PA, and
2) the individual is on record as having gained access to the MAA, and
3) the individual has authorizations for access to the requested area and material at the requested time.

Access to computers and stored data would be handled similarly. These requirements mean that the PA, MAA, and internal access controls must all be in communications with one another as well as in direct communication with physical protection personnel. A database of entry attempts is maintained by the access control system, with attempts to access unauthorized areas signaled to the safeguards system.

Equipment has been designed to minimize holdup. In addition, provision has been made to use process and accounting data to develop estimates of holdup for use in calculating inventory differences.

The materials accounting system encompasses the normal accounting practices necessary to develop current inventory listings by material type and area, maintain audit trails, record measurements, and calculate inventory difference. Calculation of inventory difference can be performed for any segment of the process from the unit process upward in scope to cover the entire facility. Measurement control functions are performed either by the accounting system or by a separate measurement control computer reporting to the accounting system. The necessary means of linking measurements with measurement control information have been provided allowing automatic calculation of the limit of error of the inventory difference.

Indicators or displays provided to the safeguards officer by the safeguards system and other components include:

1) authorization listings,
2) current accesses to areas,
3) access attempt failures (alarm),
4) transfers in progress,
5) historical inventory difference charts with control limits--for unit processes and the facility,

6) current inventory difference for each unit process,
7) measurements control charts, and
8) current inventory lists for each area (glove box).

These displays can be accessed as needed by the safeguards officer to ascertain the current status of any area within the facility, or to resolve any anomalies indicated.

Anomalies are indicated by alarms from individual systems as well as from analysis of combined information in the safeguards system. Rules have been developed to define the required sequence of activities for normal operation. When an activity occurs that does not conform to the rules, the safeguards system alerts the safeguards officer. For example, transfers from the vault may have the following required sequence:

1) process system requests an item for processing, notifying the vault computer;
2) vault computer deactivates shelf monitor for that item and activates the stacker-retriever;
3) stacker-retriever removes the item, signals for reactivation of the shelf monitor, reads the identifying information, weighs the item, performs appropriate measurements, and places the item on the trolley, time-out is started;
4) trolley is activated and moved to the Room 1 position;
5) operator in Room 1 removes the item from the trolley, reads the identifying information, and weighs the can, time-out is terminated (maximum of 10 minutes allowed for transfer), and then opens the can.

In addition to the listed events, there are the associated communications between systems for accounting, operator access to the room, measurements, trolley movements, and shelf monitoring.

Irregularities in the above routine would trigger an alarm to the safeguards officer; some examples are

1) trolley movement to a location other than Room 1,
2) the authorized operator is not present in Room 1,
3) the item removed from the vault shelf does not have the bar code for the item requested, and
4) ten minutes has elapsed and the operator has not performed the activities required to terminate the transfer.

Any of these irregularities would trigger an alarm; however, the safeguards officer or the safeguards computer may not necessarily prevent the transfer but may investigate the situation to determine if the activity is unusual but otherwise acceptable. Investigation of an anomaly may involve both automated and manual procedures.

IV. CONCLUSION

The integration of safeguards activities into an effective system that meets domestic safeguards requirements to protect against the insider threat requires careful consideration of safeguards functions and information flows. The traditional separation of safeguards activities into compartments of physical protection, materials control, and materials accounting inhibits information management and, thus, integration. "Rotating the coordinate system" of safeguards to organize activities into authorization, enforcement, and verification functions facilitates information flow. Analysis of information requirements and management of safeguards-relevant information accomplishes the integration of safeguards activities.

New facilities have the option of designing their process operations and safeguards systems in a coordinated manner, and in these cases the optimum degree of safeguards integration can be achieved with the least cost and impact on facility operations, benefiting both processing and safeguards. Existing facilities can integrate their current safeguards activities by analyzing the activities in light of authorization, enforcement, and verification functions and considering information management requirements for safeguards decisions. Any weaknesses in the system can be identified for upgrade, and any redundant activities can be eliminated, resulting in cost-effective improvements to the total system. In either case, whether designing new systems or analyzing existing ones, understanding the interface between facility operations and safeguards is critical to cost-effective integrated safeguards systems that meet modern standards of performance.

REFERENCES

1. J. W. TAPE, C. A. COULTER, and J. T. MARKIN, "The Role of Systems Studies in Safeguards: Designing Integrated Systems," Nucl. Mater. Manage., XV, 79-82 (July 1987).

2. J. T. MARKIN, C. A. COULTER, R. G. GUTMACHER, C. C. THOMAS, JR., AND W. J. WHITTY, "Design and Evaluation Methods for an Integrated Safeguards System," LA-9964, Vols. I and II, Los Alamos National Laboratory (March 1984).

3. R. PICARD, J. HAFER, AND T. MARR, "Technical Manual for the Materials Accounting with Sequential Testing (MAWST) Program," Los Alamos National Laboratory, Safeguards Systems Group draft report (1987).

4. K. CAMPBELL, G. L. BARLICH, B. FAZAL, and R. B. STRITTMATTER, "Fundamental Data Analyses for Measurement Control," LA-10811-MS, Los Alamos National Laboratory (February 1987).